ABSTRACT OF THE DISCLOSURE

A technique is provided for preserving a strong random number for use in a cryptographic security system for a processor-based device. The technique is particularly useful for restoring a random number to memory after data in the memory has been lost due to, for example, battery failure and replacement. Bits comprising a random number are automatically and periodically written to remote storage for subsequent recall, as needed, for substantially restoring the random number to the processor-based device. Further randomness also may be provided by masking in additional bits, such as those relating to other system components, the real-time clock, or the MAC address.